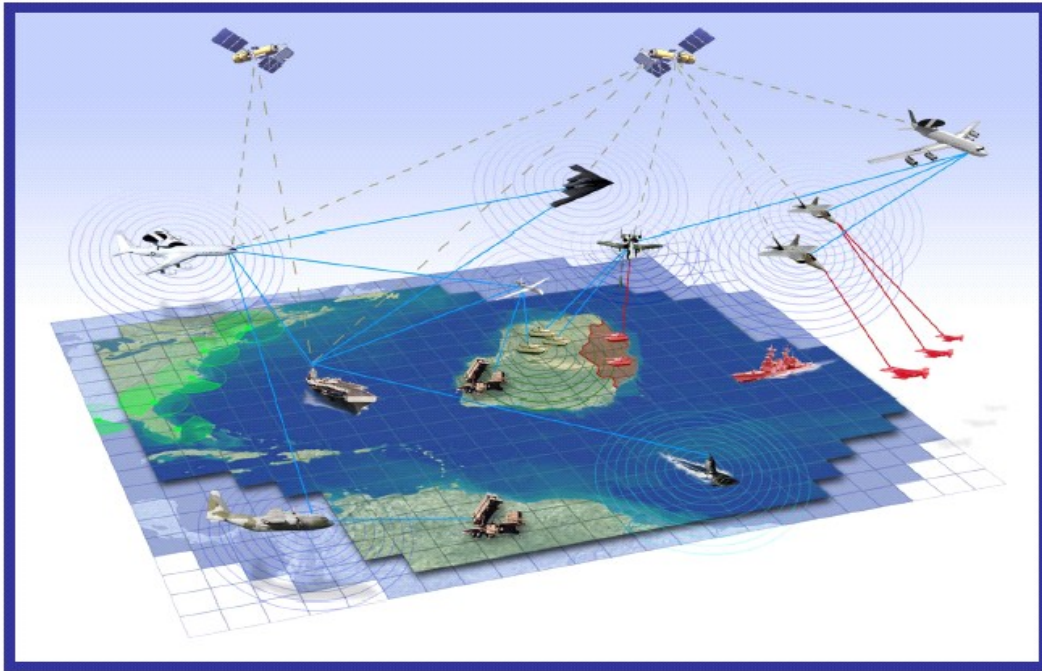# Air Force IFF Crypto Development

Identification Friend or Foe

- **Develop, Procure, Provide Mode 5 IFF Crypto to AF platforms**
  - **Single-use appliqué for Transponder or Interrogator**
  - **Dual-use appliqué for Combined Interrogator Transponder (CIT)**
  - **Stand alone unit**

- **We are funded and here to help**

- **We need to coordinate with you to make this possible**

U.S. AIR FORCE

- **Crypto Mod Role**
- **Organization**
- **Responsibilities**
- **Acquisition Strategy**
- **Schedule**
- **What's next?**
- **Summary**

U.S. AIR FORCE

CRYPTO MOD TENETS – NSA Policy 3-9

Assured Security Robustness

Programmability

Advanced Algorithms

Current Systems
(148 Families)
(>1,200,000 Crypto)

AIR

NC2

GROUND

SPACE

Global Information Grid

Cross-Cutting, Network Centric Solutions
(XX Families)

Interoperability

Releasability

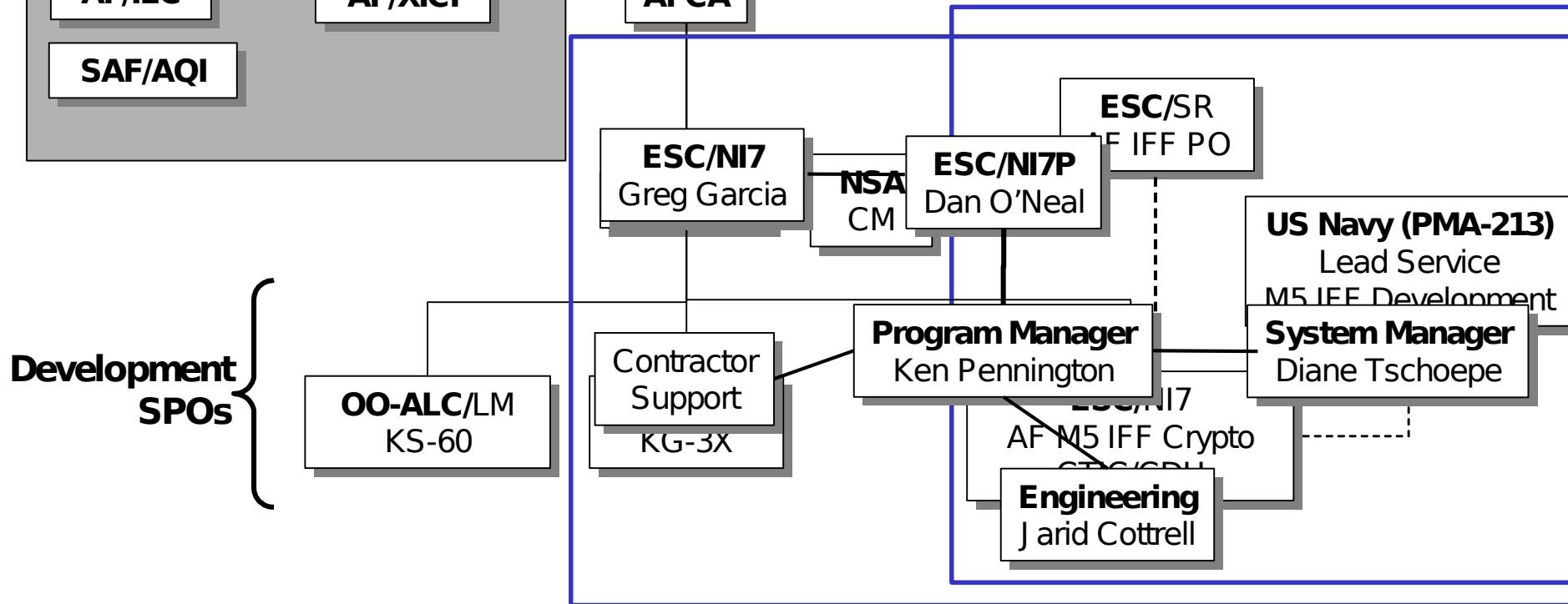**Key Management Infrastructure Compatibility**

U.S. AIR FORCE

Air Staff

| SAF/XOR | AF/XIC |
| AF/ILC | AF/XICI |
| SAF/AQI |

AF M5 IFF Crypto Development SPO Functional Structure

AFCA

ESC/SR
AF IFF PO

ESC/NI7
Greg Garcia

NSA
CM

ESC/NI7P
Dan O'Neal

US Navy (PMA-213)
Lead Service
M5 IFF Development

Development SPOs

OO-ALC/LM
KS-60

Contractor
Support
KG-3X

Program Manager
Ken Pennington

ESC/NI7
AF M5 IFF Crypto
CDS/CDU

System Manager
Diane Tschoepe

Engineering
Jarid Cottrell

C-130E / H / H1 / H2 / H3 / J	A-10A	C-40 / B / C
C-130 AMP	OA-10A	C-137C Stratoliner
AC-130H / U	B-1B Lancer	C-141 / B / C
EC-130 / EH / J	B-2A Spirit	E-4B
HC-130N / P	B-52H Stratofortress	E-9A
LC-130H / R	F-15 / A / B / C / D / E	HH-60G Blackhawk
MC-130E / H / P	F-16C Blk 25/30/32/40/42/50/52	MH-53J / M
NC-130A / H	F-16D Blk 25/30/32/40/42/50/52	MH-60G Pave Hawk
WC-130H / J	F-117A Nighthawk	TH-53A
C-135B / C / E	C-5 / A / B / C	UH-1N Iroquois
EC-135C	C-9 / A / C	KC-10A Extender
KC-135 / D / R / E / T	C-12 / C / D / F / J	U-2S/ST Dragon Lady
NKC-135E	C-21 A Learjet	VC-25A Air Force One
OC-135B Open Skies	C-26 B Metro	CL-601
RC-135 / S / U / V / X	C-29	CL-604
TC-135S / W	C-32A Boeing 757	FPS-117
WC-135W	C-37A Gulfstream V	TPS-75
	C-38 A Astra SPX	ARSR-4

Systems/Platforms Remaining
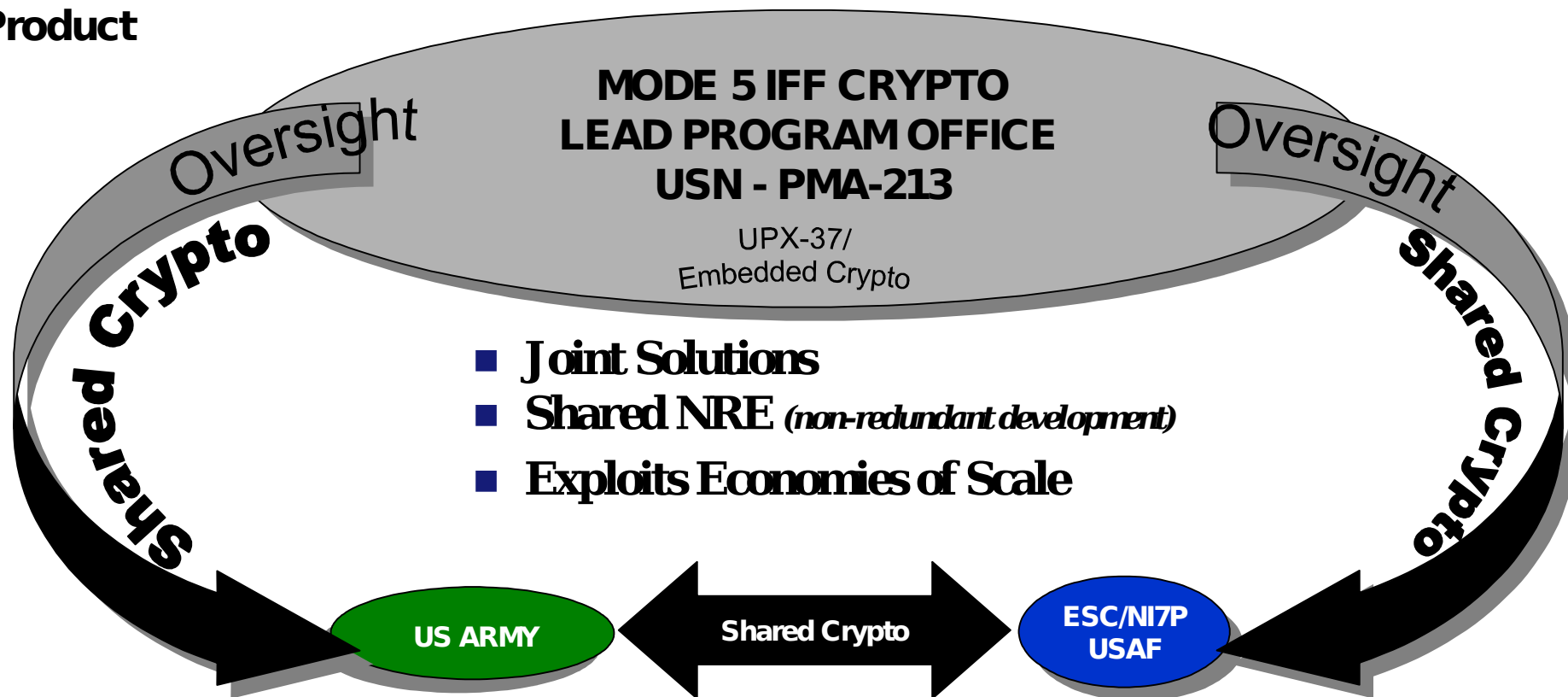
E-10	AT-38B - Trainer
CV-22A Osprey	CT-43A - Trainer
E-3B/C Sentry Block 30/35	T-1A Jayhawk - Trainer
E-8C Joint STARS	T-37B Tweet - Trainer
C-20 /B/H	T-38A Talon - Trainer
C-17A Globemaster III	T-38C - Trainer
RQ-4A Global Hawk/ Lot 1,2,3	T-3A Firefly - Trainer
RQ-1A Predator	T-41D Mescalero - Trainer
MQ-1 Predator A	T-43A - Trainer
YAL-1A Attack Airborne Laser	T-6A Texan II - Trainer
TPX-46 - Ground Radar	TC-18E - Trainer
TPX-54 - Ground Radar	

IFF Crypto Mod Relationships

JCMWG {
NSA CM
Navy CM
Army CM
Air Force CM

Policy

- -

Product

Oversight

Oversight

Shared Crypto

Shared Crypto

**MODE 5 IFF CRYPTO
LEAD PROGRAM OFFICE
USN - PMA-213**

UPX-37/
Embedded Crypto

- **Joint Solutions**
- **Shared NRE** *(non-redundant development)*
- **Exploits Economies of Scale**

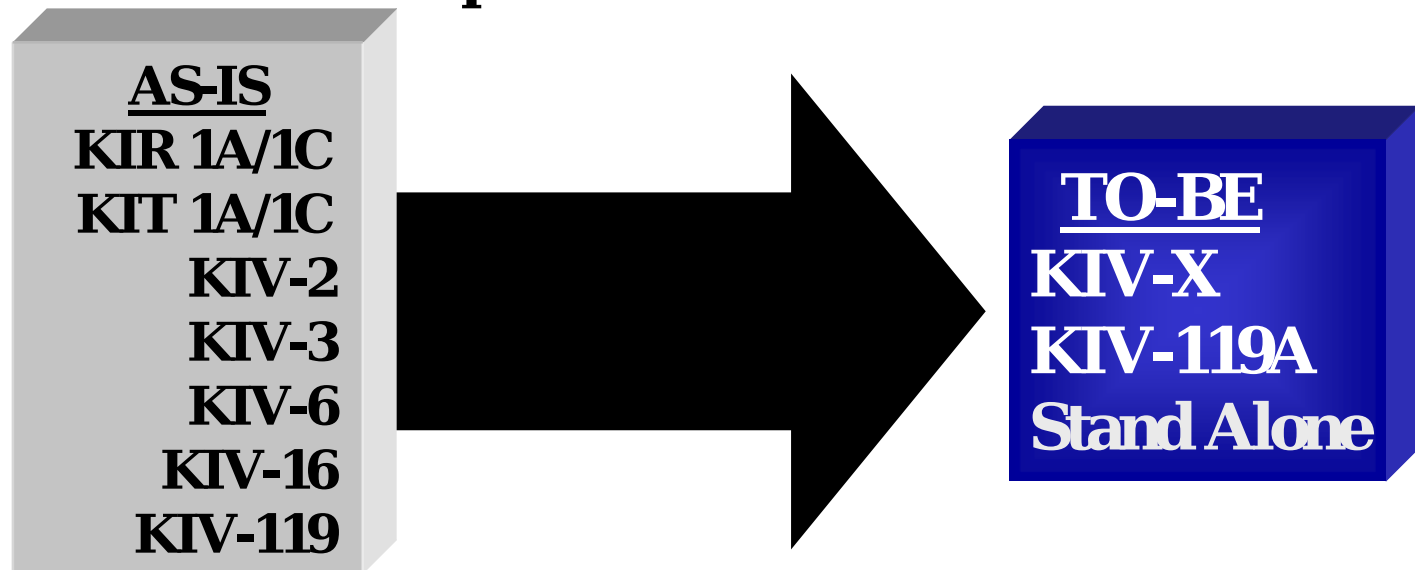**US ARMY**

Shared Crypto

**ESC/NI7P
USAF**

Integrity - Service - Excellence

- **Coordinate all AF M5 IFF Crypto - per SAF AQ**
- **Designated as the AF M5 IFF Crypto Development System Program Office**
  - **Responsible for cost, schedule, and performance of the AF IFF Crypto development/procurement**
  - **Coordinate/Conduct RDT&E efforts**
  - **Purchase and provide crypto to most platforms**
    - **For all Non-ICNIA (Integrated Communications, Navigation and Identification Architecture) platforms e.g. F/A-22, F-35 (Built into architecture)**
    - **Accomplish production planning**
- **Extensively coordinate with the IFF SPO, the Navy M5 IFF Crypto LPO, and AF platform SPOs**

Develop… Procure … Provide …

Acquisition Strategy

- **Reduce number of IFF crypto solutions**
- **Build to Crypto Interface Control Standard (CICS)**
- **Appliqué Development**
  - **Single-function**
  - **Combined-function**
- **Stand Alone Development**

AS-IS
KIR 1A/1C
KIT 1A/1C
KIV-2
KIV-3
KIV-6
KIV-16
KIV-119

TO-BE
KIV-X
KIV-119A
Stand Alone

Crypto Interface Control Standard (CICS)

- **AIMS PO is developing standard**
  - **AIMS 04-900**
  - **Complete 02 March 2004**
  - **DUAL Configuration – Single or Combined functionality**
  - **Crypto Standalone to use adapter with Standard appliqué**
- **IFF Host and Crypto vendors must build to standard**
  - **Allows development of common Crypto**
  - **Promotes vendor competition**

Maximizes cost savings... **(per unit & logistics)**

U.S. AIR FORCE
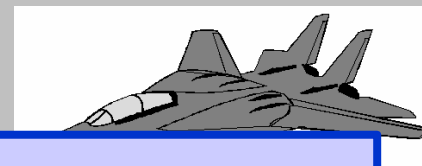
Appliqué

Embedded

Stand Alone (Cabled)

Our Focus is Appliqué / Stand-Alone

Why Appliqué?

- **Allows Form-Fit replacement**
  - **Significant reduction in platform implementation costs**
- **Economies of Scale**
  - **Multiple IFF boxes use the same crypto**
  - **Reduction in developmental costs, support costs**
- **Modular maintenance concept**
  - **Two Line Replaceable Units (LRUs)**
  - **Isolate fault to IFF or crypto**
- **Risk Reduction**
- **Mission**

COST & RISK REDUCTION

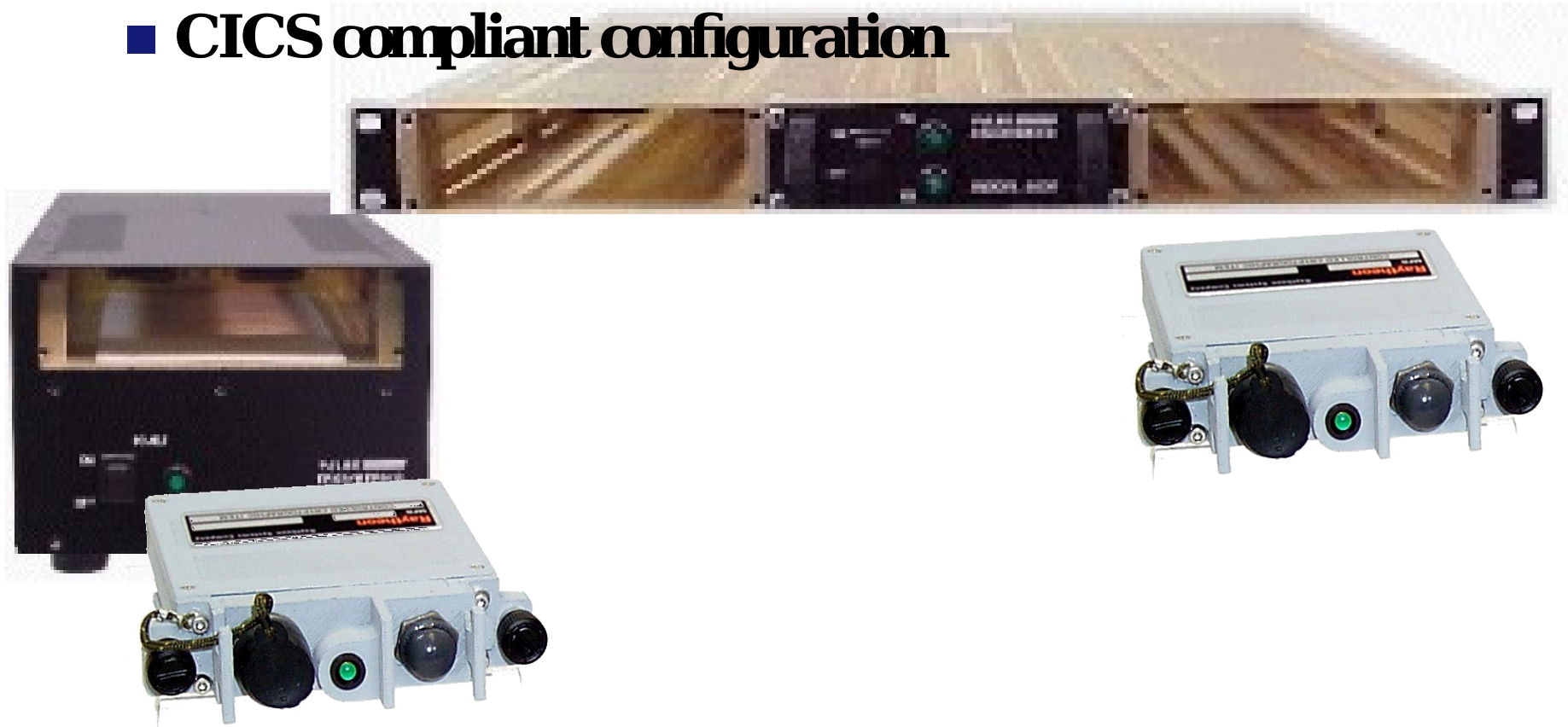**Commonality … Maintenance… Mission**

- **Transponder and Interrogator will use same appliqué**
- **Leverages Army ADI acquisition**
- **Requires form factor change for AN/APX-114 interrogator**

ESC/NI7P USAF — Shared Crypto — US ARMY

- **AF Development**
  - **Let CIT contract this year**
    - **May repackage USN embedded solution**
  - **Common crypto USN/USAF – APX-111/APX-113**
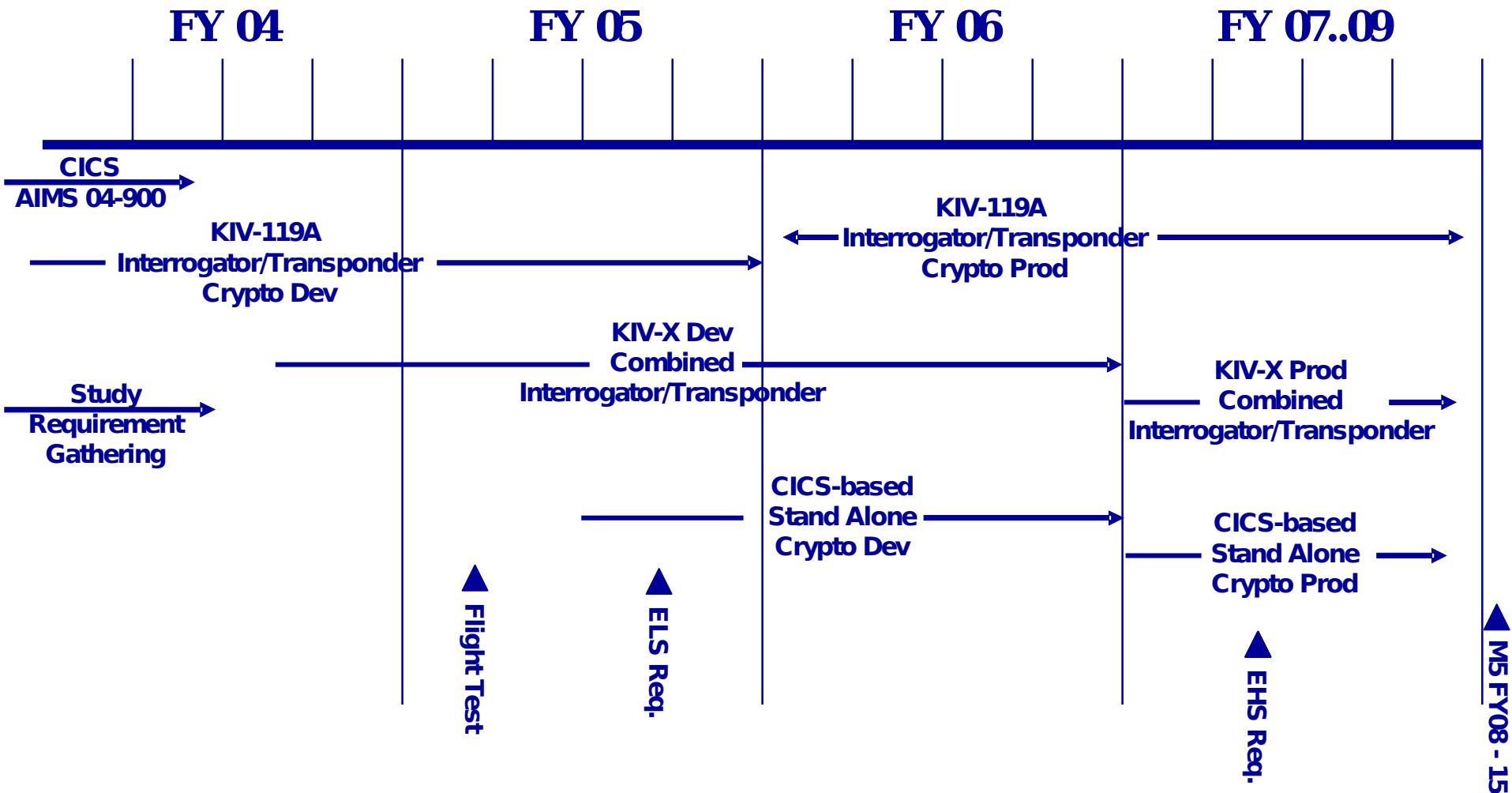
ESC/NI7P USAF ←→ Shared Crypto ←→ US NAVY

U.S. AIR FORCE

- **Re-package/adapt appliqué into stand alone package**
- **CICS compliant configuration**

Schedule

FY 04	FY 05	FY 06	FY 07..09

CICS
AIMS 04-900

KIV-119A
Interrogator/Transponder
Crypto Dev

KIV-119A
Interrogator/Transponder
Crypto Prod

KIV-X Dev
Combined
Interrogator/Transponder

KIV-X Prod
Combined
Interrogator/Transponder

Study
Requirement
Gathering

CICS-based
Stand Alone
Crypto Dev

CICS-based
Stand Alone
Crypto Prod

▲ **Flight Test**
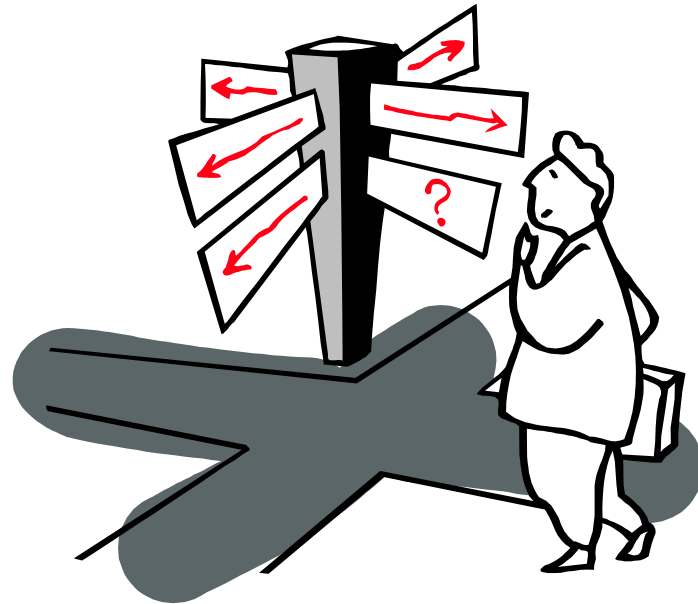
▲ **ELS Req.**

▲ **EHS Req.**

▲ **M5 FY08 - 15**

- **Increase awareness**
- **Individual follow-on meetings**
  - **Discuss platform-specific needs**
  - **Review/analyze fielding schedule**
  - **Gather additional contacts**
- **Integrate Platform SPO data into comprehensive M5 IFF Crypto strategy**
- **Let CIT contract this year**

- **NI7 to Develop/Procure/Provide M5 IFF Crypto solution to platforms**
- **Appliqué is Air Force preferred solution**
- **SPOs must coordinate crypto needs with ESC/NI7**

Bottom Line

- ◆ **We are funded! – FREE CRYPTO**
- ◆ **We are here to help!**

U.S. AIR FORCE

- Ken Pennington Program Manager (210) 977-6254 george.penningington2@lackland.af.mil

- Diane Tschoepe System Manager (210) 977-6254 diane.tschoepe@lackland.af.mil

- Jarid Cottrell Engineering (210) 977-6254 jarid.cottrell@lackland.af.mil

- Bill Blanchette Contractor Support (210) 977-6254 william.blanchette@lackland.af.mil

- Tony Perez CM Office (210) 977-5782 antonio.perez@lackland.af.mil

- FAX 969-6247 DSN 969- and last four digits.

BACK-UP SLIDES

IFF Host upgrades to Mode 5

- **Mode 4 with Mode 5 Growth Capable**
    - **Use KIT or KIR until Mode 5 upgrade**
    - **IFF host upgrade needed to be Mode 5 capable/ready**
        - **Option1 – Card and software upgrade**
        - **Option2 – Software upgrade only**
        - **Option3 – Purchase box that is already capable**
    - **Mode 5 Crypto device needed**
- **Mode 4 and Mode 5 Capable/Ready**
    - **Host runs Mode 5, no upgrade is needed**
    - **Mode 5 crypto device needed**

U.S. AIR FORCE

- **Reference – Draft AF IFF Mode 5 KMP**
  - **Net Centricity – NSA/CSS Policy 3-9 Requirement 6**
  - **Electronic Key Management System (EKMS)**
  - **Key Management Infrastructure (KMI)**
  - **End Information Assurance Unit (EIAU) Management (EM)**

- **IFF CONOPs Tiger Team**
  - **IPT to develop KMP, etc**